A Concerted Effort: The Role of the Private Sector in the context of the chapter on criminalization and procedural measures and law enforcement

Pei Ling LEE – Head Cyber Strategy & Capabilities Development

Vienna, 3 – 4 November 2022
Private Sector Cooperation in Law Enforcement

• Cooperation between states/law enforcement and the private sector are commonly referenced or alluded to in international conventions and policy instruments
  – UNTOC Article 31, UNCAC Article 12
  – UN Open-ended Intergovernmental Expert Group (IEG) to Conduct a Comprehensive Study of the Problem of Cybercrime, Seventh Session, April 2021
  – Budapest Convention on Cybercrime of the Council of Europe

• INTERPOL’s partnerships with the private sector
  – Sharing of expertise, technology and resources
  – Bridging gaps, providing vital services or capabilities that would otherwise not be available to our 195 member countries
  – Cooperation areas:
    • Data sharing, including inputs to the [INTERPOL Global Crime Trend Report](#) and regional cyberthreat assessments (e.g. [Africa](#) and [ASEAN](#))
    • Expert attachments
    • Capacity building
    • Investigation tools and platforms
Public-Private Partnerships – Project Gateway

- Partnerships: underpinning the three core pillars of INTERPOL’s Global Cybercrime Programme
- Formal data exchange agreements between INTERPOL and private-sector companies
- Robust legal and governance framework
  - The Constitution establishes fundamental rules and principles by which INTERPOL operates
  - Rules on the Processing of Data (RPD)
    Article 28 (Conditions relating to data processing by private entities) allows the establishment of data-sharing relations through cooperation agreements
  - Commission for the Control of INTERPOL’s files (CCF)
Example: **Operation Cyclone**

- 30-month transcontinental investigation and operation relating to cyber attacks against South Korean companies and US academic institutions by the Cl0p ransomware threat group
- **Arrest** of 6 members in Ukraine in June 2021
- **Seizure / confiscation** of property, computers and USD 185,000 in cash assets
- **2 Red Notices** circulated to all INTERPOL member countries (NCBs) following a request by South Korea’s cybercrime investigation division
- Assistance through **information provided by Gateway partners** (Trend Micro, Cyber Defense Institute, Kaspersky, Palo Alto Networks, Fortinet, Group-IB)
- 2 South Korea-based companies (S2W and KFSI) provided **dark web analysis** throughout the operation
Example: Operation Delilah

- Initiated by intelligence referral from Gateway partners (Group-IB, Palo Alto Networks Unit 42, Trend Micro)
- Intelligence enriched within INTERPOL’s Cyber Fusion Centre, including seconded law enforcement officials and private-sector experts
- Actionable intelligence referred to Nigeria; case coordination meetings with Australia, Canada and the United States
- Suspect’s alleged malicious online activities mapped out and tracked with ad hoc support from another private sector firm (CyberTOOLBELT)
- Arrest of the suspect, alleged to run a transnational syndicate that launched mass phishing campaigns and BEC schemes
- Example of public-private cooperation through proactive data sharing, criminal analysis, technical and live operational support
Example: Africa Cyber Surge Operation and Training

- 18 July to 5 August 2022; involving 22 member countries and AFRIPOL
- 4 cybercrime areas – malware hosting or distribution servers, defaced government websites, phishing sites, and compromised IP addresses
- **Cyber Activity Reports (CARs)** sent to countries through i-24/7 ahead of the event
- Weeks 1 and 2: Training for participating countries by Cyber Defense Africa and private company (CSI Tech) on malware investigation, cryptocurrency investigation and dark web
- Week 3: Operational execution, including takedowns of compromised infrastructure, seizures, arrests, prevention / mitigation measures where possible
- **Cybercrime Collaboration Platform – Operation** was actively used for progress updates and uploading of operational reports

**Results**

- 1000s malicious IPs identified
- Identification of individual threat actors
- Dark web market identified and taken down
- Collaboration between national entities
- Trust between INTERPOL, AFRIPOL and member countries
- ISPs identified and interacted with
Example: Digital Security Challenge

- Hybrid event (in-person and online) attended by cybercrime investigators and digital forensic specialists from 40 countries
- Collaboration with private-sector partner Cyber Defense Institute, in partnership with NEC
- Lectures and hands-on exercises on tools and techniques for investigating cybercrime organizations and infrastructures, analysis of ransomware and anonymization techniques used by illegal websites on the dark web
نشكركم جزيل الشكر على انتباهكم

Thank You  Merci-Gracias

p.lee@interpol.int

https://www.interpol.int/en/Crimes/Cybercrime